HP-UX AAA Server A.06.01 Getting Started Guide

HP-UX 11.0, 11i v1, 11i v2

Manufacturing Part Number : T1428-90058
E1004

U.S.A.

Legal Notices

The information in this document is subject to change without notice.*Hewlett-Packard makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.* Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Warranty. A copy of the specific warranty terms applicable to your Hewlett- Packard product and replacement parts can be obtained from your local Sales and Service Office.

Restricted Rights Legend. Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

HEWLETT-PACKARD COMPANY
3000 Hanover Street
Palo Alto, California 94304 U.S.A.

Use of this manual and flexible disk(s) or tape cartridge(s) supplied for this pack is restricted to this product only.

Trademark Notices. UNIX is a registered trademark of The Open Group. Internet Explorer ® is a registered trademark of Microsoft Corporation. Netscape Navigator™ is a registered trademark of Time Warner, Inc. MC/ServiceGuard® is a registered trademark of Hewlett-Packard Company. ProLDAP™ is a trademark of Interlink Networks, Inc. OpenLDAP® is a registered trademark of the OpenLDAP Foundation

Interlink Networks, Inc.
5405 Data Court, Suite 300
Ann Arbor, MI 48108
www.interlinknetworks.com

Contents

Contents

About This Document

This document provides an overview of the HP-UX AAA Server and explains how to install and start the product. The document also provides steps to basic configuration tasks for beginning users. Refer to the HP-UX AAA Server Administrator's Guide for complete HP-UX AAA Server documentation.

The document printing date and part number indicate the document's current edition. The printing date and part number will change when a new edition is printed. Minor changes may be made at reprint without changing the printing date. The document part number will change when extensive changes are made.

Document updates may be issued between editions to correct errors or document product changes. To ensure that you receive the updated or new editions, you should subscribe to the appropriate product support service. See your HP sales representative for details.

The latest version of this document can be found at `http://docs.hp.com` on the Internet and Security Solutions page.

Intended Audience

This Getting Started Guide is designed for first-time and beginning users of the HP-UX AAA Server. The objective of this guide is to allow you to quickly familiarize yourself with the basic functions of the product. Users should be familiar with the HP-UX operating system before using this guide.

New and Changed Documentation in This Edition

- Removed the various requirements, including installing and operating requirements, for each specific 6.1.x version of the HP-UX AAA Server. Refer to the HP-UX AAA Server Release Notes for the requirements of each version of the product.

Publishing History

The following table shows the printing history of this document. The first entry in the table corresponds to this document, while previous releases are listed in descending order.

Table 1 Getting Started Guide Printing History

Document Part Number	Document Release Date (month/year)	Supports Software Version	Supported OS
T1428-90058	10/04	A.06.01.x	HP-UX 11i v1, 11i v2
T1428-90049	01/04	A.06.01.x	HP-UX 11.00, 11i v1, 11i v2
T1428-90043	10/03	A.06.01.x	HP-UX 11.00, 11i v1
T1428-90026	04/03	A.06.00.08	HP-UX 11.00, 11i v1
T1428-90015	02/03	A.06.00.07	HP-UX 11.00, 11i v1
T1428-90002	06/02	A.05.01.01	HP-UX 11.00, 11i v1

What's in This Document

- Chapter 1, Introduction to AAA Server, contains an overview of product features and basic information about using the server.
- Chapter 2, Installing and Starting the HP-UX AAA Server, leads you through server installation, testing the installation, and starting the Server Manager GUI.
- Chapter 3, Basic Configuration Tasks, contains procedures that lead you through basic configuration and testing tasks.

Typographical Conventions

`monospace` Identifies files, daemons, or any other item that may appear on screen

italics Identifies titles of books, chapters, or sections

Document Advisories Different types of notes appear in the text to call your attention to information of special importance. They are enclosed in ruling lines with a header that indicates the type of note and its urgency.

NOTE	Emphasizes or supplements parts of the text. You can disregard the information in a note and still complete a task.

IMPORTANT	Notes that provide information that are essential to completing a task.

CAUTION	Describes an action that must be avoided or followed to prevent a loss of data.

Related Documents

In addition to this Getting Started Guide, HP released the following documents to support the HP-UX AAA Server A.06.01.x:

- HP-UX AAA Server A.06.01 Administrator's Guide
- HP-UX AAA Server A.06.01.02 Release Notes
- HP-UX AAA Server A.06.01.02.04 Release Notes
- HP-UX AAA Server A.06.01.02.06 Release Notes
- HP-UX AAA Server A.06.01.02.07 Release Notes
- HP-UX AAA Server A.06.01.05 Release Notes

The Administrator's Guide and the Getting Started Guide are installed with the product at `/opt/aaa/share/doc/`. You can also find these documents in the Server Manager's Help menu. The most recently released documentation for the HP-UX AAA Server is always available at `http://www.docs.hp.com` on the `Internet and Security Solutions` page.

HP Encourages Your Comments

HP encourages your comments concerning this document. We are truly committed to providing documentation that meets your needs.

Please send comments to: netinfo_feedback@cup.hp.com

Please include document title, manufacturing part number, and any comment, error found, or suggestion for improvement you have concerning this document. Also, please include what we did right so we can incorporate it into other documents.

1 Introduction to AAA Server

This chapter contains an overview of product features and basic information about using the HP-UX AAA Server.

RADIUS Overview

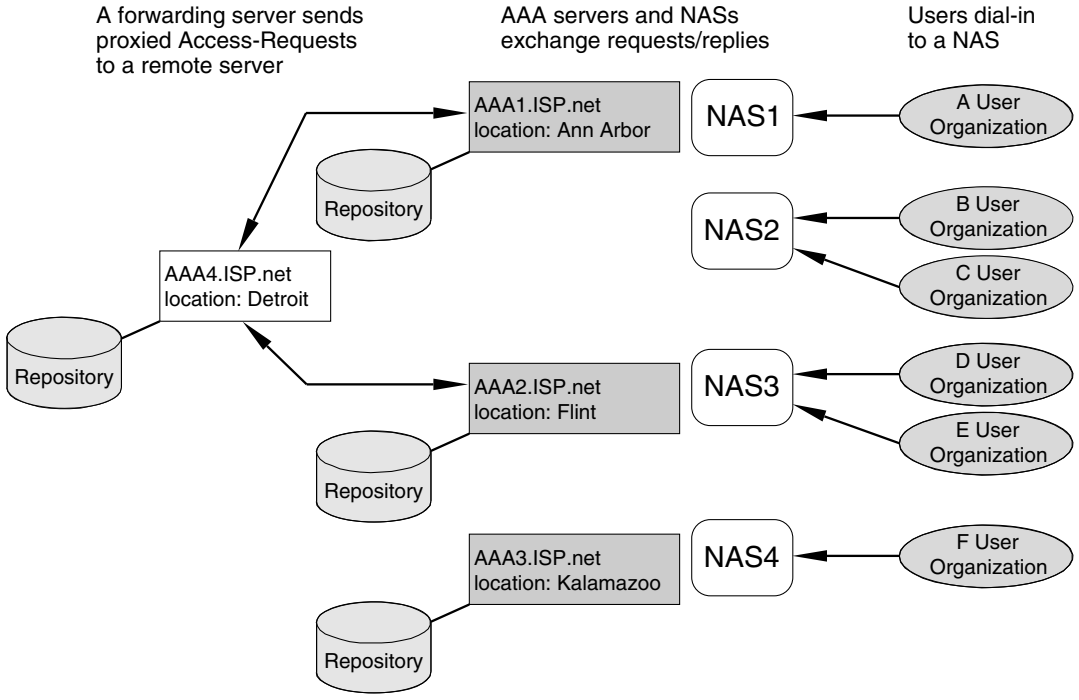
The Remote Authentication Dial In User Service (RADIUS) protocol is widely used and implemented to manage access to network services. It defines a standard for information exchange between a Network Access Server (NAS) and an authentication, authorization, and accounting (AAA) server for performing authentication, authorization, and accounting operations. A RADIUS AAA server can manage user profiles for authentication (verifying user name and password), configuration information that specifies the type of service to deliver, and policies to enforce that may restrict user access.

RADIUS Topology

The RADIUS protocol follows client-server architecture. The client sends user information to the RADIUS AAA server (in an Access-Request message) and after receiving a reply from the server acts according to the returned information. The RADIUS AAA server receives user requests for access from the client, attempts to authenticate the user, and returns the configuration information and polices to the client. The RADIUS AAA server may be configured to authenticate an Access-Request locally or to act as a proxy client and forward a request to another AAA server. After forwarding a request, it handles the message exchanges between the NAS and the remote server. A single server can be configured to handle some requests locally and to forward proxy requests to remote servers.

In Figure 1-1 on page 3 an example ISP uses four AAA servers to handle user requests. Each user organization represents a logical grouping of users (defined as a realm). Each user organization dials in to one of the ISP's servers through an assigned NAS, some of which are shared by the same groups or realm. To provide appropriate service to a customer, the server accesses user and policy information from a repository, which may be integrated with the server, may be an external application, or a database that interfaces with the server. For the HP-UX AAA RADIUS and policy server the repository information may be stored in flat text files or in an external database, such as an Oracle® database or LDAP directory server.

Figure 1-1 Generic AAA Network Topology

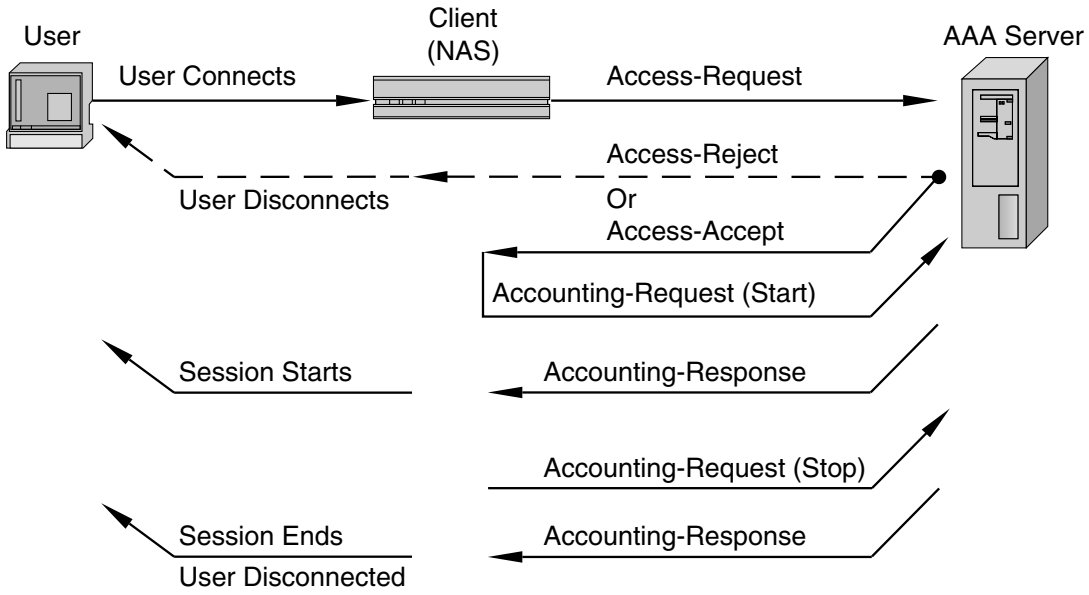


Establishing a RADIUS Session

The handling of a user request is series of message exchanges that attempts to provide the user with a network service by establishing a session for the user. This transaction can be described as a series of actions that exchange data packets containing information related to the request. Figure 1-2, Client-Server RADIUS Transaction, illustrates the details of the

transaction between a RADIUS AAA server and a client (a NAS in this example). When the user's workstation connects to the client, the client sends an Access-Request RADIUS data packet to the AAA server.

Figure 1-2 Client-Server RADIUS Transaction



When the server receives the request, it validates the sending client. If the client is permitted to send requests to the server, the server will then take information from the Access-Request and attempt to match the request to a user profile. The profile will contain a list of requirements that must be met to successfully authenticate the user. Authentication usually includes verification of a password, but can also specify other information, such as the port number of the client or the service type that has been requested, that must be verified.

If all conditions are met, the server will send an Access-Accept packet to the client; otherwise, the server will send an Access-Reject. An Access-Accept data packet often includes authorization information that specifies what services the user can access and other session information, such as a timeout value that will indicate when the user should be disconnected from the system.

When the client receives an Access-Accept packet, it will generate an Accounting-Request to start the session and send the request to the server. The Accounting-Request data packet describes the type of service being delivered and the user that will use the service. The server will respond with an Accounting-Response to acknowledge that the request was successfully received and recorded. The user's session will end when the client generates an

Accounting-Request—triggered by the user, by the client, or an interruption in service—to stop the session. Again, the server will acknowledge the Accounting-Request with an Accounting-Response.

Supported Authentication Methods

The following list describes the authentication methods the HP-UX AAA Server supports:

Password Authentication Protocol (PAP)

Not a strong authentication method to establish a connection; passwords are sent in clear text between the user and client. When used with RADIUS for authentication, the messages exchanged between the client and server to establish a PPP connection corresponds to Figure 1-2. This authentication method is most appropriately used where a plaintext password must be available to simulate a login at a remote host. In such use, this method provides a similar level of security to the usual user login at the remote host.

Challenge Handshake Authentication Protocol (CHAP)

A stronger authentication protocol to establish a connection. When used with RADIUS for authentication, the messages exchanged between the client and server to establish a PPP connection is similar to Figure 1-2. One difference, however, is that a challenge occurs between the user and NAS before the NAS sends an Access-Request. The user must respond by encrypting the challenge (usually a random number) and returning the result. Authorized users are equipped with special devices, like smart cards or software, which can calculate the correct response. The NAS will then forward the challenge and the response in the Access-Request, which the AAA server will use to authenticate the user.

Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)

An implementation of the CHAP protocol that Microsoft created to authenticate remote Windows workstations. In most respects, MS-CHAP is identical to CHAP, but there are some differences. MS-CHAP is based on the encryption and hashing algorithms used by Windows networks, and the MS-CHAP response to a challenge is in a format optimized for compatibility with Windows operating systems.

Extensible Authentication Protocol (EAP)

Like CHAP, EAP is a more secure authentication protocol to establish a PPP connection than PAP and offers more flexibility to handle authentication requests with different encryption algorithms. It allows authentication by encapsulating various types of authentication exchanges, such as MD5. These EAP messages can be encapsulated in the packets of other protocols, such as RADIUS, for compatibility with a wide range of authentication

mechanisms. This flexibility also allows EAP to be implemented in a way (LEAP, for example) that is more suitable for wireless and mobile environments than other authentication protocols. EAP allows authentication to take place directly between the user and server without the intervention by the access device that occurs with CHAP.

The following is a list of the EAP supported authentication methods you can use with the HP-UX AAA Server A.06.01:

- **Transport Layer Security (TLS)**: Uses TLS (also known as SSL) to authenticate the client using its digital certificate. Note: some wireless supplicants require specific extensions to support certificates for EAP. TLS features include: Dynamic Key Exchange; Mutual Authentication; Digital Certificate/Token Card-based Authentication; and, Encrypted Tunnelling.
- **Tunneled TLS (TTLS)**: Can carry additional EAP or legacy authentication methods like PAP, MS-CHAP, and CHAP. Integrates with the widest variety of password storage formats and existing password-based authentication systems. Wireless supplicants available for a large number of clients. TTLS features include: Dynamic Key Exchange; Mutual Authentication; Password-based Authentication; and, Encrypted Tunnelling.
- **Protected EAP (PEAP)**: Functionally very similar to TTLS, but does not encapsulate legacy authentication methods. PEAP features include: Dynamic Key Exchange; Mutual Authentication; and, Encrypted Tunnelling.
- **Message Digest 5 (MD5):** Passwords are hashed using the MD5 algorithm. Can be deployed for protecting access to LAN switches where the authentication traffic will not be transmitted over airwaves. Can also be safely deployed for wireless authentication inside EAP tunnel methods. The main feature in MD5 is Password-based Authentication.
- **Lightweight EAP (LEAP)**: For Legacy Cisco equipment only. LEAP features include: Dynamic Key Exchange; Mutual Authentication; and, Password-based Authentication.
- **Generic Token Card (GTC)**: Carries user specific token cards for authentication. The main feature in GTC is Digital Certificate/Token Card-based Authentication.
- **EAP MS-CHAP**: Passwords are hashed using a Microsoft algorithm. Can be deployed for protecting access to LAN switches where the authentication traffic will not be transmitted over airwaves. Can also be safely deployed for wireless authentication inside EAP tunnel methods. EAP-MSCHAP features include Mutual Authentication and Password-based Authentication.

RADIUS Data Packets

The Access-Request and other RADIUS data packets contain a header and a set of attribute-value (A-V) pairs, which are used by the server during the AAA transaction. The RADIUS RFC 2865 defines how vendors can extend the protocol. Encapsulation is the RFC

defined way of extending RADIUS. Conflicts can occur when the RFC is not followed. In those cases, the server can map the attributes to unique internal values for processing. For a full description of RADIUS attribute-value pairs, see the Administrator's Guide.

Shared Secret

Encrypting the transmission of the User-Password in a request is accomplished by a shared secret. The shared secret is used to sign RADIUS data packets to ensure they are coming from a trusted source. The shared secret is also used to encrypt user passwords with certain authentication methods such as PAP. The HP-UX AAA Server uses the `clients` configuration file to associate a secret to each client (or server) that is authorized to make use of its services.

Product Structure

The HP-UX AAA Server, based on a client/server architecture, consists of the following components which may be installed independently:

- HP-UX AAA Server daemon, libraries, and utilities
- The AAA Server Manager is the user interface that performs administration and configuration tasks from a client's browser for one or more AAA servers.
- AAA Server module for Oracle authentication
- Documentation

The exchange of configuration information between a remote AAA server and the AAA Server Manager program is validated by a shared secret. This secret is unique to the Server Manager and a remote AAA server. It should not be the same secret used by a AAA server and the peers that it communicates with. The exchange of information between a browser and the client program is not validated or encrypted by default, although you can configure HTTPS to secure this communication. Refer to the *HP-UX AAA Server Administrator's Guide* for more information about configuring Server Manager to run over HTTPS.

NOTE To secure the communication between the Server Manager and the HP-UX AAA Server, install the Server Manager and the HP-UX AAA Server software inside a secure network.

AAA Servers

AAA server installations include the AAA server, which performs the authentication, authorization, and accounting functions to process requests, and RMI objects. The RMI objects establish a connection and facilitate communication between the AAA server and the HP-UX Tomcat-based Serverlet Engine.

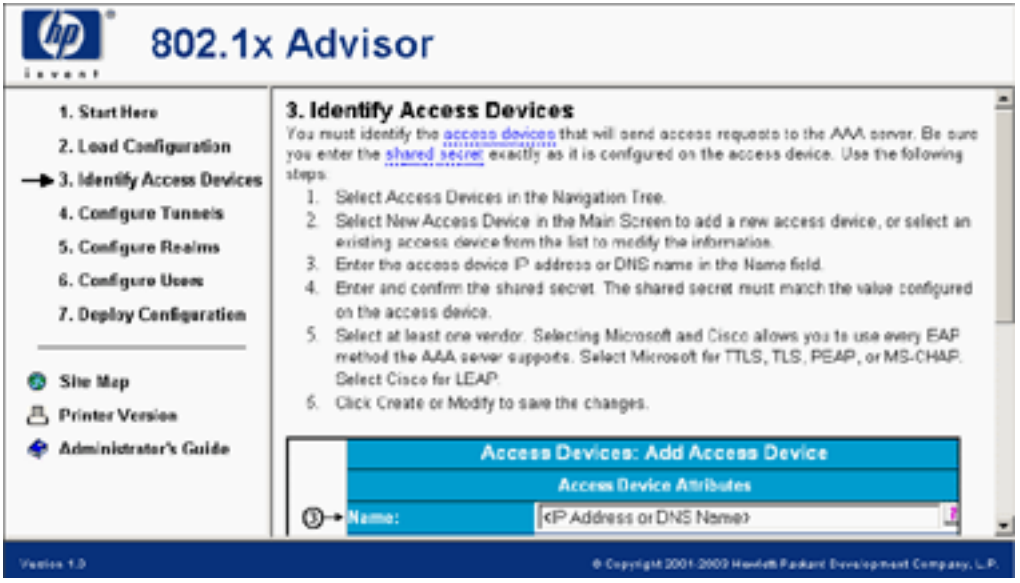
AAA Server Manager Program

The AAA Server Manager utilizes the HP-UX Tomcat-based Serverlet Engine to provide a configuration interface between a web browser and one or more AAA servers. Server Manager is used for starting, stopping, configuring, and modifying the servers. In addition, the program can retrieve logged server sessions and accounting information for an administrator.

The 802.1x Advisor

The 802.1x Advisor is an HTML tutorial/help system in the Server Manager GUI that walks you through the tasks and Server Manager screens for securing WLANs with the HP-UX AAA Server. The 802.1x Advisor provides information only—it does not edit configuration files. Follow the 802.1x Advisor and use Server Manager to create and deploy basic AAA configurations for securing WLANs. Refer to the HP-UX AAA Server Administrator's Guide for complete HP-UX AAA Server documentation. The following figure shows the 802.1x Advisor.

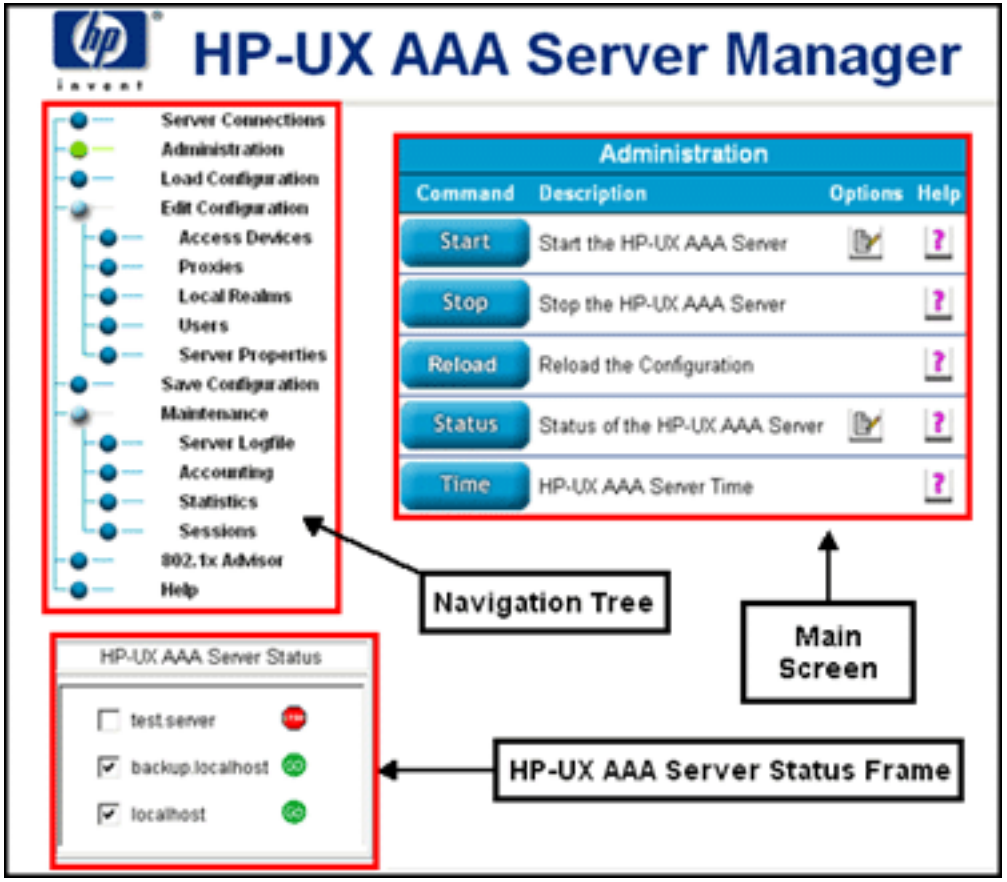
Figure 1-3 The 802.1x Advisor For Securing WLANs



Accessing the Server Manager

The Server Manager provides access to the AAA server management functions and configuration files. From a remote client workstation, administrators can access the AAA Server Manager interface through a Web browser. An administrator can create a AAA configuration for authenticating users and implementing authorization policies. In addition to creating, modifying, and deleting entries in many of the server's configuration files, an administrator may start and stop the AAA server, access the server's status and system time, retrieve information from accounting and session logs, and terminate sessions. You can access the functions that perform these operations by selecting an item from the Navigation Tree located in the left frame of the HTML page.

Figure 1-4 The Server Manager User Interface



Some advanced features of the HP-UX AAA Server cannot be configured through the Server Manager interface. For example, if you want to define session management parameters, policies, or vendor-specific attributes, you must manually edit the configuration files. Refer to the *HP-UX AAA Server Administrator's Guide* for more information.

IMPORTANT Refer to the HP-UX AAA Server Release Notes for the supported browsers for each version of the product.

NOTE The browser preferences or Internet options should be set to always compare loaded pages to cached pages.

AAA Server Architecture

The HP-UX AAA Server Architecture consists of three primary components:

- Configuration files. By editing these flat text files, with either the Server Manager user interface or with a text editor, you can provide the information necessary for the server to perform authentication, authorization, and accounting requests for configured users.
- AATV plug-ins perform discrete actions; such as initiating an authentication request, replying to an authentication request, or logging an accounting record.
- The software engine, which includes the Finite State Machine (FSM) and some associated routines. At server startup, the finite state machine reads instructions from a state table—by default the `/etc/opt/aaa/radius.fsm` text file. The state table outlines what AATV actions to call and what order to call them in.

When the server is initialized, it performs a few distinct operations. It loads and initializes the AATV plug-ins, so that actions can be executed when called by the finite state machine. It also reads the configuration files to initialize the data required for the actions to execute according to the application's requirements.

Configuration Files

The HP-UX AAA Server reads data from the following configuration files installed at `/etc/opt/aaa/` by default:

Table 1-1 HP-UX AAA Server Configuration Files

File	Description
`clients`	Information about all RADIUS clients—name, address, shared secret, type, etc.—that allows the server to recognize and communicate with the clients.
`authfile`	Authentication type parameters for defined realms.
`users`	Information about user IDs, passwords, and check/deny/reply items.

Table 1-1 HP-UX AAA Server Configuration Files (Continued)

File	Description
`<realm name>.users`	The same information as the `users` file, but this user information is associated with a particular realm. These files are only necessary to perform File type authentication for a defined realm. Realms are recognized by the realm component of the user's Network Access Identifier, for example: user@realm.com. **NOTE:** This is a user generated file, it does not ship with the product.
`decision`	Policy information for user authorization and session control based on any logical group that can be defined with A-V pairs. **NOTE:** This is a user generated file, it does not ship with the product.
`las.conf`	Defines services for session control based on realms.
`vendors`	Optional entries for vendor-specific behavior.
`dictionary`	Defines all attributes and values that may be used to build attribute-value (A-V) pairs that will be recognizable by the server. These A-V pairs contain information about requests and responses. This file also contains definitions for all the authentication types that the server recognizes.
`log.config`	Specifies the predefined session log formats to use.
`aaa.config`	Calls `engine.config` and contains properties for the following: • DHCP relay • SNMP properties • Certificate paths • Tunneling properties

Table 1-1 HP-UX AAA Server Configuration Files (Continued)

File	Description
`iaaaAgent.conf`	Specifies how often the AAA server's SNMP subagent will check to see if a master agent is active.
`EAP.authfile`	Used to configure EAP authentication for user profiles.
`db_srv.opt`	The configuration script for the `db_srv` environment variables.
`engine.config`	Called by `aaa.config`, this file stores most of the AAA server properties.

You can find out more information about these files by referring to the *HP-UX AAA Server Administrator's Guide*. Each configuration file also contains comments with examples.

AATV Plug-Ins

Define actions to perform functions, such as authenticating requests, authorizing, and logging. Built-in actions support authentication of users from information in different storage methods. The AATV plug-in files are in `/opt/aaa/aatv/`.

The Software Engine: Finite State Machine

In the Finite State Machine, a request will transition through a series of states, starting with a state that includes possible starting events. The first action specified to be called in response to an initial authentication request would return a value, an event that determines the next state to transition to. Within each state, the next action is triggered by an event (based on previous state and action and a value, typically ACK or NAK, returned by the previous action), which in turn directs the flow of the request to another state, until an End state is reached.

HP-UX AAA Server Features

General Features

- Compliant with RADIUS protocol RFC 2865 and 2866 standards
- Supports multiple vendor NASs with a single server (multi-vendor dictionary that includes Nortel®, Cisco®, Lucent®, and others)
- Configurable dictionary that allows the definition of new vendors and vendor-specific attributes and values
- Dictionary includes attributes from RFCs 2865, 2866, 2867, 2868, and 2869
- Vendor-specific attribute translation
- Configurable attribute-value pruning behavior (based on dictionary and clients file definitions)
- Various configurable (through `aaa.config`) internal queue and buffer sizes
- Persistent user session table and automatic recovery of session information after a server reload occurs
- Engine support of loadable plug-in modules

Authentication Features

- Distributed authentication (proxy) by realms (RADIUS type authentication)
- Support for PAP authentication protocol by all supported authentication types
- Support for CHAP (clear text password required in the user profile)
- Support for MS-CHAP
- Support for EAP authentication for wireless LAN access points and switches (including EAP-MD5, EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-GTC, and EAP-LEAP)
- Authentication of users with profiles defined in a flat text file that the server loads into memory (clear text or UNIX-style encrypted passwords)
- Authentication of users defined in a /etc/passwd file
- Authentication using multiple sets of user definition and realm definition files (`users` and `authfile` files) keyed by network access server (NAS)

- Supports multiple user definition (`realm`) files keyed by realm (File type authentication)
- Authentication of users defined in an LDAP server (ProLDAP™ type authentication), including support of {clear} indicator for clear text passwords
- Authentication of users defined in an ORACLE database
- UNIX bigcrypt() for users defined in a flat file or LDAP directory
- Load balancing and failover when authenticating users stored in an LDAP directory server or Oracle database

Authorization Features

- Support of simple authorization policy through check and deny attribute-value pair items specified in users files
- Support for definition of reply item attribute-value pairs in a users file
- Support of simple authorization policy through check and deny attribute-value pair items specified in realm files (File type authentication) or an LDAP directory server (ProLDAP type authentication)
- Support for definition of reply item attribute-value pairs through realm files, an LDAP directory server, or an Oracle database
- Support of complex authorization policy construction through Boolean expressions with attribute-value pair operands
- Supports simultaneous session limitation by user and by realm

Accounting Features

- Generates Merit or Livingston reference accounting detail files (accounting start and stop RADIUS messages from network access server (NAS)), known as call detail records (CDR)
- Supports distributed accounting (proxy) by realms (RADIUS type authentication)

Admin and Debug Tools/Features

- Server Manager Graphical User Interface (GUI) for managing multiple AAA servers
- 802.1x Advisor HTML help system to quickly secure WLANs with the HP-UX AAA Server
- DHCP interface for the AAA Server to assign IP addresses generated by a DHCP server
- Support for Simple Network Management Protocol (SNMP)

- "Self-signed" AAA Server digital certificates created during installation allow for a secured TLS, TTLS, and PEAP environment without having to generate your own certificates
- Generates server activity logfiles, compressed daily
- Optional debug levels for greater server log output to help debug problems
- Packaged with a RADIUS protocol client (`radpwtst`) for testing and debugging
- Packaged with a utility, (`radcheck`), to check status of server.
- Script (`las.test.sh`) tests simultaneous session control to aid in performance of session testing of the server

2 Installing and Starting the HP-UX AAA Server

This chapter leads you through the steps to install and start the HP-UX AAA Server.

Getting the HP-UX AAA Server Software

You can get the most recent version of the HP-UX AAA Server software at the HP Software Depot: `http://software.hp.com`.

Installing the HP-UX AAA Server

IMPORTANT Be sure to review the HP-UX AAA Server Release Notes before installation. The Release Notes list the requirements for each release, including: installation, patch, and browser requirements.

You can access the Release Notes online at: `http://docs.hp.com/hpux/internet/index.html#HP-UX%20AAA%20Server%20%28RADIUS%29`

The following components are installed when you install the HP-UX AAA Server:

- AAA Server binaries, libraries, and utilities
- RMI objects that facilitate communication from the AAA server to Server Manager
- AAA server AATV module for authentication

Perform the following steps to install the HP-UX AAA Server:

Step 1. Log in to your system as root.

Step 2. Verify the product requirements are installed.

Step 3. Verify the required patches are installed.

Step 4. Download the AAA Server depot file from `http://www.software.hp.com` and move it to `/tmp`

Step 5. Verify you downloaded the file correctly: `# swlist -d -s /tmp/<AAA Server>.depot`

Step 6. Stop any active Tomcat processes. Use `/opt/hpws/tomcat/bin/shutdown.sh` to stop Tomcat.

Step 7. Install the AAA Server: `# swinstall -s /tmp/<AAA Server>.depot`

NOTE If the installation is not successful, an error message is displayed. The cause of the failure will appear at the end of `/var/adm/sw/swagent.log` file.

Starting the HP-UX AAA Server

NOTE Refer to the *Securing the HP-UX AAA Server* section in the *HP-UX AAA Server Administrator's Guide* for information on securing your HP-UX AAA Server.

Use the following steps to start the HP-UX AAA Server and the Server Manager graphic user interface:

Step 1. Enter the following command: `# export JAVA_HOME=/opt/java1.4`

Step 2. Start the RMI objects to allow the AAA server software to communicate with Server Manager. Use the following command: `# /opt/aaa/remotecontrol/rmistart.sh`

Step 3. Start the HP-UX Tomcat-based Serverlet Engine to allow a web browser to connect to it. Use the following command: `# /opt/hpws/tomcat/bin/startup.sh`

Step 4. Point your web browser to the following URL to manage the HP-UX AAA Server with the Server Manager interface: `http://<IP-Address or FQDN>:8081/aaa`

NOTE The default Server Manager username is `tomcat`. The default Server Manager password is `tomcat`.

Step 5. Select Administration in the Navigation Tree. Verify the AAA server you want to start is selected in the Server Status Frame. Click the Start button.

Starting and Stopping the RMI Objects

- Start = `/opt/aaa/remotecontrol/rmistart.sh`
- Stop = `/opt/aaa/remotecontrol/rmistop.sh`
- Status = `# netstat -a |grep 7790`

Starting and Stopping Tomcat

- Start = `/opt/hpws/tomcat/bin/startup.sh`
- Stop = `/opt/hpws/tomcat/bin/shutdown.sh`
- Status = `# netstat -a |grep 8081`

Testing the Installation

To quickly test the server installation, you will use Server Manager to add a loopback connection to a AAA server, start the server, and then check its status for a response. Use the following steps to test the server installation:

Step 1. Connect to Server Manager and start the AAA server. See "Starting the HP-UX AAA Server" on page 22.

Step 2. Select the Server Connections link from the Navigation Tree and then select the Connect to Server link.

Step 3. Enter the values for your server in the `Add Connection` screen that appears and select Create:

Name — The identifying string of a remote server.

Domain Name or IP Address — The IP address (in dotted-quad notation) or valid Domain Name System (DNS) host name of the AAA server that the connection maps to.

Step 4. Verify the server is listed and selected in the Server Status frame.

Step 5. Select the Administration link from the Navigation Tree.

Step 6. Select Start.

Step 7. Verify the server started. A green "GO" icon in the Server Status frame indicates the server is running.

Step 8. Verify the server is selected in the Server Status frame and then select the Status option.

Step 9. Check Server Manager's Message Frame for the status reply. The following reply at the bottom of the Message Frame indicates the server is running correctly:

```
"<server name> (port#)" is responding
```

NOTE If you did not receive this message, refer to the Troubleshooting chapter in *HP-UX AAA Server Administrator's*.

Step 10. Verify your HP-UX AAA Server is installed and operating correctly by using the testing user (named `test_user`) created during installation. After `test_user` is authenticated and the AAA server sends an Access-Accept, the client sends an Accounting-Request to start the session. After the session is terminated, the client sends an Accounting-Request stop message to stop the session logging and the AAA server writes the session information to a file.

a. Enter the following command:

```
# /opt/aaa/bin/radpwtst -s localhost -i 10.0.0.1 -l 1  test_user
```

This command simulates an Access-Request from port 1 of a NAS with an IP address of 10.0.0.1. When prompted for a password, enter: `password`. The command should return the following output:

```
'test_user' authentication OK
```

b. Enter the following command:

```
#  /opt/aaa/bin/radpwtst -c 4 -s localhost -i 10.0.0.1 -l 1 -u ppp -:Acct-Status-Type=Start
test_user
```

This command simulates an Accounting-Request start message, activating the users's PPP session. The command should return the following output:

```
Accounting Response received
```

c. Enter the following command:

```
#  /opt/aaa/bin/radpwtst -c 4 -s localhost -i 10.0.0.1 -l 1 -u ppp -:Acct-Status-Type=Stop
test_user
```

This command simulates an Accounting-Request stop message, terminating the users's session. The command should return the following output:

```
Accounting Response received
```

d. View the session logs for `test_user's` start and stop accounting messages by selecting Accounting in Server Manager's Navigation Tree and clicking Display.

IMPORTANT HP recommends removing `test_user` or changing it's default password before deploying your HP-UX AAA Server in a production environment. See the *Securing the HP-UX AAA Server* section in the *HP-UX AAA Server Administrator's Guide*.

Installation Defaults

The HP-UX AAA Server can be run as root user, however non-root user is recommended.

A user and group, both named `aaa`, will be created during installation. The HP-UX AAA Server can be run as non-root user, using the default aaa user created during installation, or any other user who is part of the `aaa` group.

IMPORTANT Do not remove the default login aaa and group aaa created during installation, even if you prefer not to use them.

Table 2-1 File Locations Upon Installation

Directory	File
`/opt/aaa/aatv`	Server modules and plug-ins
`/opt/aaa/bin`	Server daemons and utilities: • `db_srv`: Oracle client daemon for authentication • `las.test.sh`: script to create simulated sessions for testing • `radcheck`: AAA Server test utility (like the ping command) • `raddbginc`: controls server debug output • `radiusd`: AAA Server executable • `radpwtst`: AAA test client utility • `start_db_srv`: script to start the Oracle client daemon • `stop_db_srv`: script to stop the Oracle client daemon
`/opt/aaa/examples/config`	Finite state machine, group policy example files: • `*.fsm`: sample finite state machine (FSM) tables • `*.grp`: sample decision files

Table 2-1 File Locations Upon Installation (Continued)

Directory	File
/opt/aaa/examples/oracle	• create.sql: SQL script to create Oracle users table • delete.sql: Sample SQL script to delete Oracle user records • insert.sql: Sample SQL script to add Oracle user records
/opt/aaa/examples/proldap	ProLDAP schema and sample LDIF files
/opt/aaa/lib — Note that shared library files have .so file extensions on HP-UX 11i v2.0 (B.11.23)	Shared libraries: • libradlib.sl: contains functions that interface with the main server • librpilib.sl: contains functions for programs and utilities • libjniAgents.sl: contains functions for Server Manager.
/opt/aaa/newconfig	Default configuration files. Files residing here are copied to /etc/opt/aaa directory during installation.
/etc/opt/aaa/security/	Directory containing a unique set of “self-signed” digital certificates created during installation.
/opt/aaa/share/man/man5 and ~/man1m	Directories where man pages are installed
/opt/aaa/share/doc/	Directory containing Administrator’s and Getting Started guides.

Table 2-1 File Locations Upon Installation (Continued)

Directory	File
/etc/opt/aaa	Configuration files: • aaa.config: runtime and tunneling configuration file • authfile: realm to authentication-type mapping file • clients: client to shared secret mapping file • db_srv.opt: configuration script for db_srv environment variables • dictionary: definition file required by radiusd • las.conf: authorization and accounting configuration file • log.config: session logging configuration file • radius.fsm: external FSM table for the server • users: holds user security profiles and reply items • vendors: holds IANA numbers and other vendor specific details • engine.config: Called by aaa.conf, this file stores most of the AAA server properties • EAP.authfile: Used to configure EAP authentication for user profiles • iaaaAgent.conf: Specifies how often the AAA server's SNMP subagent will check to see if a master agent is active • aaa.config.license: Do not alter this file • RADIUS-ACC-SERVER-MIB.txt: Text file describing RADIUS Accounting MIB definitions. • RADIUS-AUTH-SERVER-MIB.txt: Text file describing RADIUS Authentication MIB definitions.

The following table lists the files generated during operation and located in `/var/opt/aaa/` by default:

Table 2-2 Files Generated During Operation

Directory	File
`/acct/session.yyyy-mm-dd.log`	Default session accounting logs, Merit style
`/data/session.las`	Currently active sessions Session log file
`/ipc/*.sm`	Shared memory files related to the interface used for some authentication types. **IMPORTANT:** You must not alter or delete the shared memory (`*.sm`) files. The server will not operate correctly if the files are changed or removed from the `ipc` directory.
`/logs/logfile`	The server log file
`/logs/logfile.yyyymmdd`	Compressed daily or weekly log files
`/radacct/*`	For session accounting logs in Livingston call detail records directory style format (not generated by default configuration)
`/run/radius.pid`	Contains the process id (pid) for the server.

Commands, Utilities, & Daemons

Table 2-3 Commands, Utilities, & Daemons

Command	Description
db_srv	The db_srv daemon performs Oracle database access operations for authentication on behalf of one or more remote HP-UX AAA Servers.
radcheck	Sends a RADIUS status and protocol requests to a AAA server and display the replies. Receiving the reply confirms that the HP-UX AAA Server is operational. radcheck can be invoked on any host by any user, however the HP-UX AAA server will return more information to registered clients.
raddbginc	Sets debug logging level for currently running HP-UX AAA Server. Turn debugging on and off or set the level of output while the AAA Server is running.
radiusd	A daemon process that services user authentication and accounting requests from RADIUS clients. Authentication and accounting requests come to radiusd in the form of UDP packets conforming to the RADIUS protocol. It runs as a daemon that can be started from the Server Manager GUI, command line, or through an inetd service. radiusd determines the action to take when receiving RADIUS requests based upon a finite state machine (FSM) loaded into memory when radiusd is started. The FSM is configurable, but static after startup.
radpwtst	A utility used to simulate a RADIUS client when troubleshooting or validating configuration for the HP-UX AAA Server. It will prompt for the user password (when not supplied by the -w option.) If the request to the AAA server succeeds, radpwtst displays authentication OK on standard output. Otherwise, radpwtst displays <userid> authentication failed.
start_db_srv.sh	Script to start Oracle authentication client daemon db_srv.
stop_db_srv.sh	Script to stop db_srv daemon and its child process(es).
las.test.sh	Script to create simulated sessions for testing.

UnInstalling the HP-UX AAA Server Software

Use the following steps to uninstall the HP-UX AAA Server:

Step 1. Select Administration in the Navigation Tree. Verify the AAA server you want to stop is selected in the Server Status Frame. Click the Stop button to stop the server.

Step 2. From the command line, stop the RMI objects and Tomcat. Refer to "Starting and Stopping the RMI Objects" and "Starting and Stopping Tomcat" on page 22 for more information.

NOTE You may have to enter the following command if you have not already: `# export JAVA_HOME=/opt/java1.4`

Step 3. Stop the `db_srv` server if it is running. Use the following command to determine if db_srv is running: `$ ps -ef |grep db_srv`

You can stop `db_srv` servers with the `/opt/aaa/bin/stop_db_srv.sh` script.

Step 4. Remove all files residing in the `/var/opt/aaa/` and `/opt/hpws/tomcat/webapps/aaa/aaalog/` subdirectories.
Logout anyone using HP-UX AAA Server administrator login "`aaa`".

Step 5. As root user, enter "`swremove T1428AA`" or "`swremove`" at the command prompt to invoke the standard HP-UX GUI to select T1428AA bundle for removal. See the `swremove` man page for more information on this command.

3 Basic Configuration Tasks

This chapter explains a few basic configuration tasks. Refer to the *HP-UX AAA Server Administrator's Guide* for complete information on configuring the HP-UX AAA Server.

Storing User Profiles

The user information that determines how an access request is authenticated and authorized is configured in a profile as a set of A-V pairs. These user profiles are grouped by realm and may be stored in flat text files or an external source such as an Oracle database or and LDAP server. Realms are recognized by the realm component of a user's Network Access Identifier. If you have a small AAA deployment without several realm-specific configurations, you can define a default realm and store it in the `users` file.

Storing User Profiles in the Default Users File

When the AAA server receives a request, before it checks for profiles grouped by realms, it first checks the default users file for a matching profile. Use the following steps to store user profiles in the default users file:

Step 1. Access the Server Manager.

Step 2. Load the configuration from the appropriate AAA server by selecting the `Load Configuration` link from the Navigation Tree.

Step 3. Select the Users link from the Navigation Tree.

Step 4. Select the New User link.

Step 5. The User Attributes screen will appear. In the User Name text box, enter the name of the user profile.

IMPORTANT You must enter the user's fully-qualified name when adding to the default users file. For example, enter `user1@organization.com` instead of only entering `user1`.

Step 6. Select Local from the Authentication Type list to authenticate the user with the authentication method configured for their realm. Selecting options other than Local will supersede the authentication method configured for the user's realm and define a specific authentication method for that individual user.

Step 7. Enter a password for the user and confirm it by entering it again.

Step 8. Choose how you want to store the user's password by selecting a hashing method in the Password Hashing Mechanism field. Select Plain Text to be compatible with most client password hashing methods. If you prefer not to use Plain Text, be sure

the method you choose is compatible with the client password hashing method. The following table lists the supported client password hashing methods and each storage hash you should use for each method:

Table 3-1 Password Hashing Compatibility

Client Password Hash	Storage Hash
PAP	Any
MSCHAP	NT Hash or Plain Text
MD5	MD5 or Plain Text
GTC Static	Any

Step 9. You may enter values in the remaining fields to control the users session. These fields are optional and correspond to RADIUS A-V pairs that are explained in more detail in the *HP-UX AAA Server Administrator's Guide.*

Step 10. Select the Create button.

Step 11. Select `Save Configuration` from the Navigation Frame. If you have multiple remote servers, you will prompted to select and confirm which servers you wish to add the access device entry to.

CAUTION Save Configuration will save the entire server configuration (access devices, proxies, local realms, users, and server properties) to the servers you specify.

Grouping Users by Realm

While the HP-UX AAA Server can authenticate an individual user, you may want to authenticate and provision a group of users according to a common criteria, like an authentication type. One method of grouping users is according to the realm that they belong to. A realm is derived from a user's Network Access Identifier, for example: `name@sample.com` where `sample.com` is the realm. Use the following steps to store user profiles in a flat text file grouped by realm:

Step 1. Access Server Manager.

Step 2. Select the Local Realms link from the Navigation Tree and then select the New local realm link

Step 3. In the Name field, enter the realm name.

Step 4. Select Authentication from the Realm Type drop-down list.

Step 5. Select Users File in the User Profile Storage drop-down list.

Step 6. Select the Users Profile Grouped by Realm button in the User Storage Parameters field. Identify a file to store the user information for the realm by entering a name in the File Name box. The AAA server adds a `.users` extension to the value you enter in the File Name box. Do not enter a path or use the / character.

Step 7. In the Security Methods field, choose the authentication methods to authenticate the users from the realm.

Step 8. Select the Create button.

Step 9. Return to the Local Realms screen to add user profiles to the realm.

Step 10. From the Local Realms screen, select the following icon for the realm that you wish to add user profiles for:

Step 11. From the Users screen select the New User link.

Step 12. In the User Name text box, enter the name of the users profile.

Step 13. In the Password text box, enter the value to match to the value to compare to the Password attribute value in the request. Confirm the password by entering it again.

Step 14. You may enter values in the remaining fields to control the users session. These fields are optional and correspond to RADIUS A-V pairs that are explained in more detail in the “A-V Pairs” chapter of *HP-UX AAA Server Administration and Authentication Guide*.

Step 15. Select the Create button in the User Attributes screen.

Step 16. Repeat steps 9 to 13 for each user profile you wish to add to the realm.

Step 17. Repeat these steps to add additional realms and groups of users.

Step 18. Select `Save Configuration` from the Navigation Frame. If you have multiple remote servers, you will prompted to select and confirm which servers you wish to add the access device entry to.

CAUTION Save Configuration will save the entire server configuration (access devices, proxies, local realms, users, and server properties) to the servers you specify.

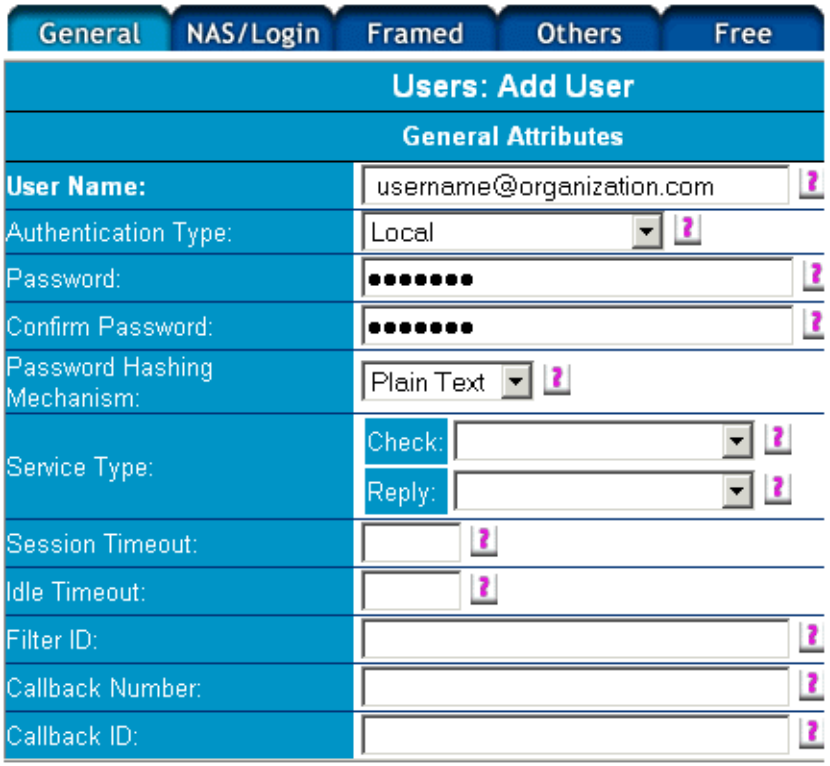
Adding and Modifying Users

User profiles associate information with a user name for authentication and authorization. This information is defined by attribute-value pairs. The server configuration must include profiles for all the users that can access services through the AAA server. If a user profile is not included in the configuration, the server will reject the users access request.

Profiles may be stored in flat text files or an external source. The Users screen allows you to add a new user, modify an existing user, or delete an existing user from a text file. This screen is accessed by selecting the Users link from the graphic interfaces Navigation Tree.

When adding a new user profile to the server configuration or modifying an existing entry, you supply values for the user profile attributes through a form's fields. This form is tabbed according to groups of attribute-value pairs. Initially, the General tab is active.

Figure 3-1 Server Manager's General User Attributes



User Name: Value to compare to the User-Name attribute value in the request. It must be less than 64 characters. &, “, ~, \, /,%, $, ‘, and space characters may not be used.

IMPORTANT You must enter the user’s fully-qualified name when adding to the default users file (using the Users link in the Navigation Tree): for example, enter `user1@organization.com` instead of only entering `user1`.

Authentication Type:
Use this field to supersede the Authentication type specified in the user’s realm. Selecting Local will use the authentication method specified by the user’s realm.

Password and Confirm Password:
Enter the user’s password and confirm it by entering it again.

Password Hashing Mechanism:
Choose how you want to store user passwords by selecting a hashing method. Select Plain Text to be compatible with most client password hashing methods. If you prefer not to use Plain Text, be sure the password storage hashing method you choose is compatible with the client password hashing method as described in Table 3-1 on page 33.

The remaining fields and tabs in Define Users screen allow you to specify two types of user profile attributes: check items and reply items.

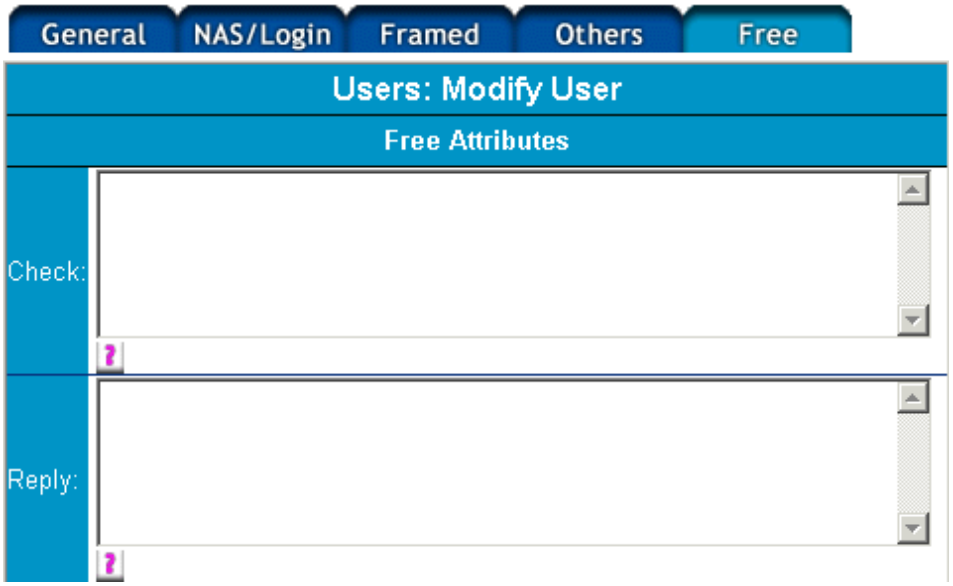
Check Items: An optional list of zero or more attribute-value pairs, delimited by white space. These items indicate various attribute values that the server will compare to the corresponding attribute values in the Access-Request.

Reply Items: Reply items generally get returned to configure the client for the user’s session. They include information like PPP configuration values, the name of the host that the user wishes to connect to, or an optional packet filter name.

Each of the fields on the first four tabs (General, NAS/Login, Framed, and Others) corresponds to an attribute that can be used in a user profile as a check or reply item. When specifying attribute values through these tabs, all A-V pairs that may ordinarily be used as either a check or a reply item in a server configuration are automatically added as a reply item, unless the Free tab is used.

There are many more attributes, including vendor-specific attributes, that can be added to a user profile. The Free tab allows you to enter any of these attributes in the Check and Reply list boxes.

Figure 3-2 Server Manager's Free User Attributes Screen



To add attributes to the list boxes, follow the Attribute = Value syntax. A-V pairs may be listed one per line. When adding a new user profile, you select the Create button to submit it to the AAA Server Manager. When modifying an existing profile, you select the Modify button to submit changes to the user profile. In either case if each field contains a valid value, the profile will be created or modified; otherwise, an error message is displayed. You can always select the Cancel button and return to the Users screen without making any changes to your server configuration.

Session Logging and Monitoring

You can view the log files that record the details of each AAA transaction or the session logs that record information about each user's session. You can also access information for active sessions and manually terminate a session if necessary.

These functions can be accessed by selecting the `Maintenance` menu items from the Server Manager Navigation Tree. When you use any of these functions, you will retrieve information from all servers selected in the Server Manager's Server Status section.

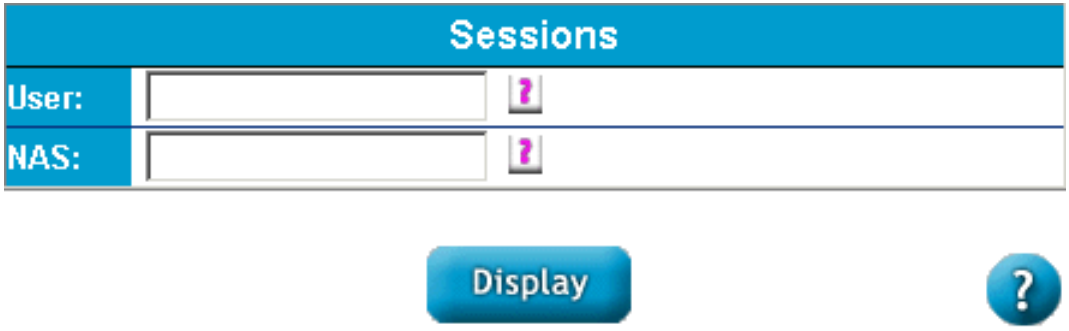
Viewing User Session

After a user is successfully authenticated and the AAA server sends an Access-Accept, the access device will send an Accounting-Request message to start the session. The AAA server stores information about the session in an active session record. When the users session is terminated, the client sends an Accounting-Request message to stop the session. When a AAA server receives the stop message, it clears its active record for the session and writes the session information to a file.Use the following steps to display session information for a particular user:

Step 1. Through the Server Manager interface, select the Sessions link from the Navigation Tree located in the left frame of the browser

Step 2. Enter search parameters in the Session Filter screen that appears. Retrieved session will be restricted to the specified search parameters.

Figure 3-3 Sessions Search Filter Screen



Step 3. Select the Display button. The AAA server manager will display a list of active sessions.

Step 4. Select a session. The AAA server manager will display the attributes for the selected session.

Step 5. Select the OK button when you are done reading the session.

Stopping a Session

This procedure is intended for sessions that were terminated on the access device but are maintained as active by the AAA server.

Step 1. Follow the “Viewing User Session” on page 39 procedure.

Step 2. Select the Stop button from the Session Attributes screen. The AAA server will clear its record of the active session, but no action is taken by the access device.

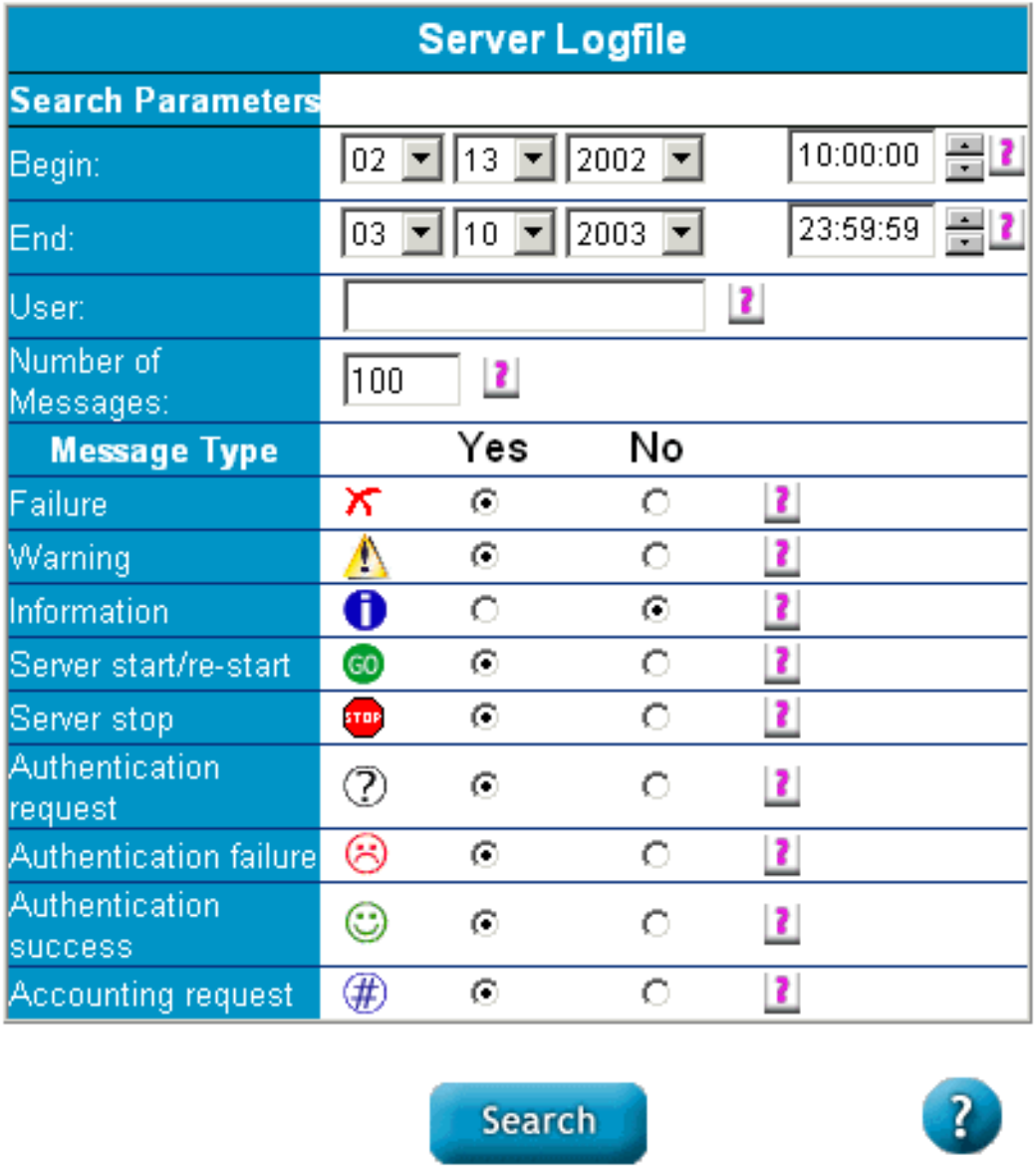
Viewing Server Logfiles

The log file of the AAA server contains all the information concerning the functioning of the server such as: start/stop of the server, all of the RADIUS requests, and some internal events. Selecting the `Server Logfile` link in Server Manager’s Navigation Tree allows you to retrieve information from log files. The data is automatically stored each day in a different file. They are available as long as the corresponding files are still on the disk.

- `/var/opt/aaa/logs/logfile`: the server log file
- `/var/opt/aaa/logs/logfile_part<01-09>.yyyymmdd`: compressed daily log file

NOTE	If the logfile exceeds its size limit (as configured in the File Size Property in the Server Properties link), a new logfile for that day will be created and identified by the `part<01-09>` portion logfile file name string.

Figure 3-4 Server Manager's Logfile Screen



Search Parameters

You can filter what dates and times to retrieve from the logfile.

Table 3-2 Filter Parameters for Searching Logfiles

Option	Description
Begin (server time)	The date and time of the session to begin retrieving data from.
End (server time)	The date and time of the last session to retrieve data from.
User	Limits the result of the search command to messages related to a specific user. For example, you may wish to find why a user is not able to authenticate.
Number of Messages	Limits the result of the search command to the specified number of messages.

NOTE You can filter what data to retrieve according to the type of messages. For each message type, you indicate whether the message type should or should not be retrieved by selecting the Yes or No radio buttons. Refer to the *HP-UX AAA Server Administration and Authentication Guide* for more information.

Viewing Server Statistics

Selecting the `Statistics` link from Server Manager's Navigation Tree allows you to retrieve a count of events that occurred on the AAA server within a time range. The statistics are displayed using a bar graph.

Figure 3-5 Server Manager's Statistics Screen

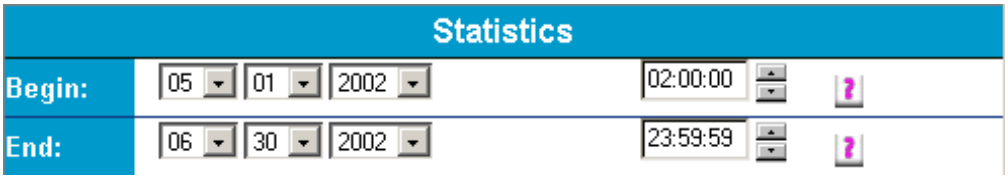


Table 3-3 Statistic Search Parameters

Option	Description
Begin (server time)	The date and time of the session to begin retrieving data from.
End (server time)	The date and time of the last session to retrieve data from.

Securing WLANs with the HP-UX AAA Server

The HP-UX AAA Server provides security framework to support EAP authentication mechanisms for WLAN users. The HP-UX AAA Server allows authentication of wireless users with password or non-password based mechanisms and supports dynamic key generation for data encryption between the access point and wireless stations.

IMPORTANT To configure the HP-UX AAA Server to secure WLANs, refer to the 802.1x Advisor and the *HP-UX AAA Server Administrator's Guide*. The 802.1x Advisor is available from the Server Manager interface and walks you through the steps and screens for securing WLANs with the HP-UX AAA Server.

4 Glossary of Terms

802.1x Advisor

The 802.1x Advisor is an HTML tutorial/help system in the Server Manager GUI that walks you through the tasks and Server Manager screens for securing WLANs with the HP-UX AAA Server.

AAA

Abbreviation for Authentication, Authorization, and Accounting.

AAA Server

A software application that performs authentication, authorization, and accounting functions.

Accounting

Logging session and usage information for session control and billing purposes

Access-Accept

The AAA server returns an Access-Accept to the client when an Access-Request is valid. The Access-Accept will contain A-V pairs that specify what services the authenticated user is authorized to use.

Access-Challenge

The AAA server returns an Access-Challenge to the client when it is necessary to issue a challenge that the user must respond to. The client will resubmit the request with the user-supplied information to the AAA server.

Access-Reject

The AAA server returns an Access-Reject to the client when an Access-Request is invalid.

Access-Request

Created by the client, the Access-Request contains A-V Pairs, such as the user's name, password, and ID of the client. The client submits the Access-Request to an AAA server. If the server can validate the client, the server will attempt to match a user entry in its database with information in the Access-Request to authenticate the user.

Administrator

Special user, known by the system on which the AAA server is running and is able to configure and to manage the AAA server.

Application Service Provider

Third-party entities that manage and distribute software-based services and solutions to customers across a wide area network from a central data center, abbreviated as ASP.

ASP

Application Service Provider.

Attribute-Value Pair

The RADIUS protocol defines things in terms of attributes. Each attribute may take on one of a set of values. When a RADIUS packet is exchanged among clients and servers, one or more attributes and values are sent pair wise from the client to the server. For the AAA Server software, all valid attributes and values are listed in the dictionary file, abbreviated as A-V pair.

Authentication

The process of identifying and proving the identity of an entity, for example, a user, a network client, or a network server.

Authorization

The process of determining what types of activities is permitted. Usually, authorization is in the context of authentication; once users are authenticated, they may be authorized different types of access or activity.

A-V Pair

Attribute-value pair.

Challenge Handshake Authentication Protocol

Log-in security procedure for dial-in access. Rather than send an unencrypted password, a random number is sent to the client as a challenge. The challenge is one-way hashed with the password, and the result is sent back to the server. The server does the same with its copy of the password and verifies that it gets the same result to authenticate the user, abbreviated as CHAP.

CHAP

See *Challenge Handshake Authentication Protocol*.

Client

NAS, proxy server, or other networking device that uses the AAA server services to authenticate and authorize users.

Common Open Policy Service

A query and response protocol that can be used to exchange policy information between a policy server (Policy Decision Point or PDP) and its clients (Policy Enforcement Points or PEPs, such as a router), abbreviated as COPS.

COPS

See *Common Open Policy Service*.

Dialed Number Identification Service

Each request is authenticated locally or forwarded to a remote server according to the number called to access a network service.

DNIS

See *Dialed Number Identification Service*.

EAP

Extensible Authentication Protocol. Described in RFC 2284.

Finite State Machine

The Finite State Machine is the component of the AAA Server software that controls the flow of access request authentication and accounting request handling, abbreviated as FSM.

Forwarding Server

The AAA server that receives an Access-Request from a client and forwards that request to another AAA server for authentication.

FSM

See *Finite State Machine*.

GTC (Generic Token Card)

Carries user specific token cards for authentication. The main feature in GTC is Digital Certificate/Token Card-based Authentication.

Hint

When a user requests access to a service of a specific configuration, a client may provide this information in an Access-Request as a hint to the AAA server. The server may reject the request based on the hints or supply the service as specified by the hints, by the server's configuration, or by a combination of the hints and the server's configuration.

IETF

See *Internet Engineering Task Force*.

Integrated Services Digital Network

A digital internet access line using copper phone lines.

Interlink

Used to connect multiple AAA servers in a fabric with SLAs and to establish policies among them.

Internet Engineering Task Force

Internet standards setting organization.

Internet Protocol

A Layer 3 (network layer) protocol that contains addressing information and some control information that allows packets to be routed, abbreviated as IP.

Internet Research Task Force

A group associated with IETF focusing on research rather than standards.

Internet Service Provider

Communications service company that provides Internet access and services to its customers. ISPs range in size from small independents serving a local calling area to large, established telecommunications companies, abbreviated as ISP.

IP

See *Internet Protocol*.

IRTF

See *Internet Research Task Force*.

ISP

Internet service provider.

ISDN

See *Integrated Services Digital Network*.

LAS

See *Local Authorization Server*.

LDAP

See *Lightweight Directory Access Protocol*.

Lightweight Directory Access Protocol

Used for directories providing naming, location, management, security, and other services for Internet networking, abbreviated as LDAP.

Lightweight Extensible Authentication Protocol

Supports and manages the dynamic Wired Equivalent Privacy (WEP) key exchange between Cisco Aironet 802.11x wireless LAN clients and access points, abbreviated as LEAP.

LEAP

See *Lightweight Extensible Authentication Protocol*.

Local Authorization Server

A local authorization server is the HP-UX SERVER code that authorizes, accounts, and bill users based on realms, abbreviated as LAS.

Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP)

An implementation of the CHAP protocol that Microsoft created to authenticate remote Windows workstations. In most respects, MS-CHAP is identical to CHAP, but there are a few differences. MS-CHAP is based on the encryption and hashing algorithms used by Windows networks, and the MS-CHAP response to a challenge is in a format optimized for compatibility with Windows operating systems.

NAS

See *Network Access Server*.

Navigation Tree

Refers to the navigation links on the left side of the Server Manager GUI.

Network Access Server

A device that interfaces telephony circuits to the network, abbreviated as NAS.

PAP

See *Password Authentication Protocol*.

Password Authentication Protocol

A simple password protocol that transmits a user name and password across the network, unencrypted, abbreviated as PAP.

PEAP (Protected EAP)

Functionally very similar to TTLS, but does not encapsulate legacy authentication methods. PEAP features include: Dynamic Key Exchange; Mutual Authentication; and, Encrypted Tunnelling.

Point-to-Point Protocol

The standard protocol for dial-up networking. The family of standards covers many aspects including authentication, encryption, compression, addressing, multi-protocols, etc., abbreviated as PPP.

Policy

A very broadly used term. To the AAA server, it means the conditionally applicable set of attribute-value pairs that an AAA protocol, such as RADIUS, may support. HP-UX SERVER policies are simple or complex decisions that control the authentication, authorization, and accounting process for a user's access request.

PPP

See *Point-to-Point Protocol*.

Protocol

A set of rules established between two devices to allow communications to occur.

Proxy

The mechanism that allows one system to mediate between two other systems in response to protocol requests. A RADIUS server can act as a proxy client and forward an Access-Request to another AAA server for authentication. As a proxy client, the server would mediate the requests and replies between the client where the Access-Request originated from and the server that the request was forwarded to.

RADIUS

See *Remote Access Dial In User Service*.

RADIUS Client

A NAS or other device that sends requests to an AAA server.

RAS

See *Remote Access Server*.

Realm

A realm is a logical group of users, who usually can be authenticated using one particular method. Grouping users into realms simplifies the management of those users in a distributed environment. For example, an ISP's users may be from different organizations located in different cities. Each organization already has one way or another to authenticate its users and each corresponds to a realm. Each realm would be responsible for managing its users, providing authentication and authorization for their access requests.
A realm has a name that looks very much like a domain name, but they bear different meanings. Realms are only used by the AAA Server to determine where an authentication request should be sent and what kind of authentication to request, etc. Naming a realm with its domain name simplifies things for the users, since their access ids will then look the same as their e-mail addresses. A realm may also have multiple aliases, providing a way to shorten long realm names.

Remote Access Dial In User Service

An authentication and accounting protocol defined by the IETF in a series of RFCs, abbreviated as RADIUS.

Remote Access Server

A service that allows remote clients running Microsoft Windows or Windows NT to dial in to a network, abbreviated as RAS.

Remote Server

In the context of a proxy Access-Request, the remote server is the AAA server that receives the request from the forwarding server. The remote server authenticates the request and sends a reply to the forwarding server.

Request For Comment

The basis for an IETF standard, abbreviated as RFC.

RFC

See *Request For Comment*.

SAT

See *Simultaneous Access Token*.

Server Manager

A Web-based graphical user interface which provides an interface between an administrator and the AAA servers. In addition to creating, modifying, and deleting entries in many of the server's configuration files, an administrator may start and stop the AAA server, access the server's status and system time, retrieve information from accounting and session logs, and terminate sessions.

Service

The RADIUS client provides a service to the dial-in user, such as PPP or Telnet.

Session

Each service provided by the client to a dial-in user constitutes a session, with the beginning of the session defined as the point where service is first provided and the end of the session defined as the point where service is ended. A user may have multiple sessions in parallel or series if the RADIUS client supports that feature.

Simple Network Management Protocol (SNMP)

Provides a mechanism for a centrally located management workstation to monitor the activity of remote computers and network services.

Simultaneous Access Token

The concept of token helps define and enforce policies in regard to modem pool sharing among various participating institutions. A simultaneous access token is required when a user accesses a non-priority modem. Tokens are allocated to realms and are grouped into pools. The total number of tokens a realm has is defined by the HP-UX Server so that the LAS may control simultaneous use, abbreviated as SAT.

SLA

Service Level Agreement.

SLS

Service Level Specification.

Token

See *Simultaneous Access Token*.

Token Pool

A token pool contains a number of tokens belonging to some organization and having a given name. These tokens may be shared among one or more realms.

Tunneling

A secure connection between a client workstation and an intranet or other network, that provides a VPN to a user. This connection may be a voluntary tunnel initiated by the client or a compulsory tunnel initiated during authentication by a server or other dedicated network equipment.

TLS (Transport Layer Security)

Uses TLS (also known as SSL) to authenticate the client using its digital certificate. Note: some wireless supplicants require specific extensions to support certificates for EAP. TLS features include: Dynamic Key Exchange; Mutual Authentication; Digital Certificate/Token Card-based Authentication; and, Encrypted Tunnelling.

TTLS (Tunnelled-Transport Layer Security)

Can carry additional EAP or legacy authentication methods like PAP and CHAP. Integrates with the widest variety of password storage formats and existing password-based authentication systems. Wireless supplicants available for a large number of clients. TTLS features include: Dynamic Key Exchange; Mutual Authentication; Password-based Authentication; and, Encrypted Tunnelling.

Users

Individuals whom the AAA server must authenticate and authorize before by they can access an organization’s service, such as Internet access through an ISP.

VPN

See *Virtual Private Network*.

Virtual Private Network

A network service offered by public carriers in which the user is provided a network that in many ways appears as if it is a private network (user-unique addressing, network management capabilities, dynamic reconfiguration, etc.) but which, in fact, is provided over the carrier's public network facilities, abbreviated as VPN.

Index

W